

UNITED STATES DISTRICT COURT

for the

Eastern District of California

FILED

Oct 18, 2021

CLERK, U.S. DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA

In the Matter of the Search of)
A MAC BOOK PRO, SERIAL NUMBER:)
C02PXMFCG8WN; AND AN IPHONE, SERIAL)
NUMBER: G6TX31CCJCL8, CURRENTLY)
LOCATED AT A STORAGE LOCKER IN THE)
UNITED STATES PROBATION OFFICE IN ELK)
GROVE, CALIFORNIA)

Case No. 2:21-sw-0800 KJN

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

SEE ATTACHMENT A, attached hereto and incorporated by reference.

located in the Eastern District of California, there is now concealed (*identify the person or describe the property to be seized*):

SEE ATTACHMENT B, attached hereto and incorporated by reference

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §§ 1030(a)(5)(A), 1030(c)(4)(C)	Knowingly causing the transmission of a program information code, or command, and as a result of such conduct, intentionally causing damage without authorization to a protected computer

The application is based on these facts:

SEE AFFIDAVIT, attached hereto and incorporated by reference.

- ☐ Continued on the attached sheet.
☐ Delayed notice days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Heriberto Cadena

Applicant's signature


FBI Special Agent Heriberto Cadena

Printed name and title

Sworn to before me and signed telephonically.

Date: 10/18/2021

City and state: Sacramento, California


KENDALL J. NEWMAN
UNITED STATES MAGISTRATE JUDGE

UNITED STATES DISTRICT COURT

for the

Eastern District of California

In the Matter of the Search of)
 A MAC BOOK PRO, SERIAL NUMBER:)
 C02PXMFCG8WN; AND AN IPHONE, SERIAL)
 NUMBER: G6TX31CCJCL8, CURRENTLY)
 LOCATED AT A STORAGE LOCKER IN THE)
 UNITED STATES PROBATION OFFICE IN ELK)
 GROVE, CALIFORNIA)

Case No.

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

SEE ATTACHMENT A, attached hereto and incorporated by reference.

located in the Eastern District of California, there is now concealed (*identify the person or describe the property to be seized*):

SEE ATTACHMENT B, attached hereto and incorporated by reference

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §§ 1030(a)(5)(A), 1030(c)(4)(C)	Knowingly causing the transmission of a program information code, or command, and as a result of such conduct, intentionally causing damage without authorization to a protected computer

The application is based on these facts:

SEE AFFIDAVIT, attached hereto and incorporated by reference.

- ☐ Continued on the attached sheet.
☐ Delayed notice days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



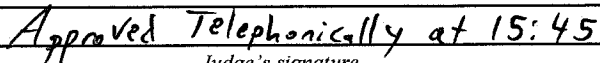
Applicant's signature

FBI Special Agent Heriberto Cadena

Printed name and title

Sworn to before me and signed telephonically.

Date: 10/18/2021



Judge's signature

City and state: Sacramento, California

Kendall J. Newman, U.S. Magistrate Judge

Printed name and title

PHILLIP A. TALBERT
Acting United States Attorney
PAUL HEMESATH
Assistant United States Attorney
501 I Street, Suite 10-100
Sacramento, CA 95814
Telephone: (916) 554-2700
Facsimile: (916) 554-2900

Attorneys for Plaintiff
United States of America

IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA

In the Matter of the Search of:

A MAC BOOK PRO, SERIAL NUMBER:
C02PXMFCG8WN; AND AN IPHONE,
SERIAL NUMBER: G6TX31CCJCL8,
CURRENTLY LOCATED AT A STORAGE
LOCKER IN THE UNITED STATES
PROBATION OFFICE IN ELK GROVE,
CALIFORNIA

CASE NO.

AFFIDAVIT IN SUPPORT OF AN APPLICATION
UNDER RULE 41 FOR A WARRANT TO
SEARCH DEVICES

I, Heriberto Cadena, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the FBI, and have been since March 6th, 2016. I am currently assigned to the Sacramento Division Field Office, Cyber Squad, which investigates matters related to computer intrusions (i.e. “hacking”), fraud and related activity in connection with access devices and fraud perpetrated over the Internet. In the course of my employment at the FBI, I have investigated federal criminal violations related to cyber intrusions, including but not limited to illegal darknet

1 activity, cyber fraud, ransomware, drug trafficking, and crimes against children. During the course of
2 my employment as a Special Agent, I have executed and participated in multiple search and arrest
3 warrants. As a result, I have seized and reviewed numerous forms of digital media for evidence of a
4 crime. In addition to training at the FBI Academy, Quantico, Virginia, I have completed numerous job-
5 related training courses, including cyber-related training programs. Moreover, I am a federal law
6 enforcement officer who is engaged in enforcing criminal laws, such as all sub-sections of Title 18,
7 United States Code 18 U.S.C. sections 1028 (identity fraud), 1029 (access device fraud), and aiding and
8 abetting, conspiracy, and attempt to commit the criminal acts listed above..

9 3. This affidavit is intended to show only that there is sufficient probable cause for the
10 requested warrant and does not set forth all of my knowledge about this matter.

11 **II. IDENTIFICATION OF THE DEVICES TO BE EXAMINED**

12 4. The property to be searched is: A MAC BOOK PRO, SERIAL NUMBER:
13 C02PXMXXCG8WN; AND AN IPHONE, SERIAL NUMBER: G6TX31CCJCL8, hereinafter the
14 “Devices.” The Devices are currently located at A STORAGE LOCKER IN THE UNITED STATES
15 PROBATION OFFICE IN ELK GROVE, CALIFORNIA.

16 5. The applied-for warrant would authorize the forensic examination of the Devices for the
17 purpose of identifying electronically stored data particularly described in Attachment B.

18 **III. PROBABLE CAUSE**

19 6. The FBI continues to investigate alleged violations of 18 U.S.C. §§ 1030(a)(5)(A),
20 1030(c)(4)(C) – knowingly causing the transmission of a program information code, or command, and
21 as a result of such conduct, intentionally causes damage without authorization to a protected computer,
22 by Matthew Keys, a former employee of Comstock’s Magazine.

23 7. On or about February 13, 2020, an employee at Comstock’s Magazine (“Comstock’s”)
24 discovered that a password to Gmail account associated with the magazine’s YouTube account—
25 comstocksmag@gmail.com—no longer functioned. Shortly thereafter, the employee found that links
26 associated with videos on the YouTube account were broken. Comstock’s employees found that the
27 videos had been deleted from the YouTube channel. The deleted content consisted of approximately 47
28 videos and the statistics associated with the channel (views, subscribers, etc.), although the exact number

1 and titles are not known in their entirety. The channel was originally created in May of 2011 and had
2 accumulated approximately 692 subscribers before it was deleted. Based on the timing of the last
3 known access to the intact videos and the date that they were discovered deleted, the videos were erased
4 sometime between February 7 and February 13, 2020.


5 8. In response, Comstock's employees collected information about the Gmail account and
6 the missing video clips. Based on data obtained from the digital accounts associated from the incident,
7 employees suspected that Matthew Keys—whose employment at Comstock's had terminated on January
8 23, 2020—was responsible for the deleted videos.

9 9. On February 9, 2020, a user had caused a new password to be created based on a two-
10 step verification code that was sent to the email address: mkeys@comstocksmag.com, as is set forth on
11 the following page (captured by a Comstock's employee):
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28




1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20

Ways we can verify it's you

These can be used to make sure it's really you signing in or to reach you if there's suspicious activity in your account



Recovery phone	(530) 507-8380	>
Recovery email	mkeys@comstocksmag.com	>
Security question	What year was Comstock's founded	>

	Password changed	California, USA - February 9, 2:54 AM
	Recovery email deleted	California, USA - February 9, 2:53 AM
	New sign-in on Apple iPhone	California, USA - February 9, 2:50 AM

21 10. Comstock's employees also verified that the dates above were consistent with the time
22 during which the content was deleted, and that the phone number listed was Keys's Google Voice
23 number.

24 11. Comstock's employees also suspected that Keys was responsible for the deletion of the
25 videos because on January 23, 2020, Keys separated from Comstock's under contentious circumstances.
26 Furthermore, they had learned that Keys had been previously convicted of conspiracy to destroy data—
27 which belonged to his then-employer—four years before in the Eastern District of California.

28 12. The United States Probation Office kept records of Keys's computer activity from

1 February of 2020. The records were created from screenshot software that was required to be installed
2 on one of Keys's computers a result of his then-ongoing supervised release. Those records showed that
3 Keys had been accessing sites related to Comstock's magazine and sites using
4 mkeys@comstocksmag.com as a user name (including the Comstock's Facebook site, an iCloud
5 account, and a 1Password account) at around 2:00 a.m., on February 9, 2020.

6 13. The devices are currently in the possession of the United States Probation Office. They
7 were seized as a result of a lawful search of Keys's residence, pursuant to the terms of his supervised
8 release. Therefore, while the FBI might already have all necessary authority to examine the Devices, I
9 seek this additional warrant out of an abundance of caution to be certain that an examination of the
10 Devices will comply with the Fourth Amendment and other applicable laws.

11 14. The Devices are currently in storage at A STORAGE LOCKER IN THE UNITED
12 STATES PROBATION OFFICE IN ELK GROVE, CALIFORNIA. In my training and experience, I
13 know that the Devices have been stored in a manner in which its contents are, to the extent material to
14 this investigation, in substantially the same state as they were when the Devices first came into the
15 possession of the FBI.

16 IV. TECHNICAL TERMS

17 15. Based on my training and experience, I use the following technical terms to convey the
18 following meanings:

- 19 a) Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is
20 a handheld wireless device used for voice and data communication through radio signals.
21 These telephones send signals through networks of transmitter/receivers, enabling
22 communication with other wireless telephones or traditional "land line" telephones. A
23 wireless telephone usually contains a "call log," which records the telephone number,
24 date, and time of calls made to and from the phone. In addition to enabling voice
25 communications, wireless telephones offer a broad range of capabilities. These
26 capabilities include: storing names and phone numbers in electronic "address books;"
27 sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and
28 storing still photographs and moving video; storing and playing back audio files; storing

1 dates, appointments, and other information on personal calendars; and accessing and
2 downloading information from the Internet. Wireless telephones may also include global
3 positioning system (“GPS”) technology for determining the location of the device.

4 b) IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric
5 address used by computers on the Internet. An IP address is a series of four numbers,
6 each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer
7 attached to the Internet computer must be assigned an IP address so that Internet traffic
8 sent from and directed to that computer may be directed properly from its source to its
9 destination. Most Internet service providers control a range of IP addresses. Some
10 computers have static-that is, long-term-IP addresses, while other computers have
11 dynamic-that is, frequently changed-IP addresses.

12 c) Internet: The Internet is a global network of computers and other electronic devices that
13 communicate with each other. Due to the structure of the Internet, connections between
14 devices on the Internet often cross state and international borders, even when the devices
15 communicating with each other are in the same state.

16 16. Based on my training, experience, and research, I know that the Devices have
17 capabilities that allow it to serve as a container of relevant data and location. In my training and
18 experience, examining data stored on devices of this type can uncover, among other things, evidence
19 that reveals or suggests who possessed or used the devices.

20 **V. ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

21 17. Based on my knowledge, training, and experience, I know that electronic devices can
22 store information for long periods of time. Similarly, things that have been viewed via the Internet are
23 typically stored for some period of time on the devices. This information can sometimes be recovered
24 with forensics tools.

25 18. There is probable cause to believe that things that were once stored on the Devices may
26 still be stored there, for at least the following reasons:

27 a) Based on my knowledge, training, and experience, I know that computer files or
28 remnants of such files can be recovered months or even years after they have been

downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b) Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c) Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d) Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

19. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a) Data on the storage media can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging

1 systems can leave traces of information on the storage medium that show what tasks and
2 processes were recently active. Web browsers, e-mail programs, and chat programs store
3 configuration information on the storage medium that can reveal information such as
4 online nicknames and passwords. Operating systems can record additional information,
5 such as the attachment of peripherals, the attachment of USB flash storage devices or
6 other external storage media, and the times the computer was in use. Computer file
7 systems can record information about the dates files were created and the sequence in
8 which they were created.

- 9 b) Forensic evidence on a device can also indicate who has used or controlled the device.
10 This “user attribution” evidence is analogous to the search for “indicia of occupancy”
11 while executing a search warrant at a residence.
- 12 c) A person with appropriate familiarity with how an electronic device works may, after
13 examining this forensic evidence in its proper context, be able to draw conclusions about
14 how electronic devices were used, the purpose of their use, who used them, and when.
- 15 d) The process of identifying the exact electronically stored information on a storage
16 medium that are necessary to draw an accurate conclusion is a dynamic process.
17 Electronic evidence is not always data that can be merely reviewed by a review team and
18 passed along to investigators. Whether data stored on a computer is evidence may
19 depend on other information stored on the computer and the application of knowledge
20 about how a computer behaves. Therefore, contextual information necessary to
21 understand other evidence also falls within the scope of the warrant.
- 22 e) Further, in finding evidence of how a device was used, the purpose of its use, who used
23 it, and when, sometimes it is necessary to establish that a particular thing is not present on
24 a storage medium.
- 25 f) I know that when an individual uses an electronic device, the individual's electronic
26 device will generally serve both as an instrumentality for committing the crime, and also
27 as a storage medium for evidence of the crime. The electronic device is an
28 instrumentality of the crime because it is used as a means of committing the criminal

1 offense. The electronic device is also likely to be a storage medium for evidence of
2 crime. From my training and experience, I believe that an electronic device used to
3 commit a crime of this type may contain: data that is evidence of how the electronic
4 device was used; data that was sent or received; and other records that indicate the nature
5 of the offense.

6 20. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the
7 warrant I am applying for would permit the examination of the devices consistent with the warrant. The
8 examination may require authorities to employ techniques, including but not limited to computer-
9 assisted scans of the entire medium, that might expose many parts of the devices to human inspection in
10 order to determine whether it is evidence described by the warrant.

11 21. Manner of execution. Because this warrant seeks only permission to examine devices
12 already in law enforcement's possession, the execution of this warrant does not involve the physical
13 intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize
14 execution of the warrant at any time in the day or night.

15 ///

16 ///

17 ///

18 ///

19 ///

20 ///

21 ///

22 ///

23 ///

24 ///

25 ///

26 ///

27 ///

28 ///

VI. CONCLUSION

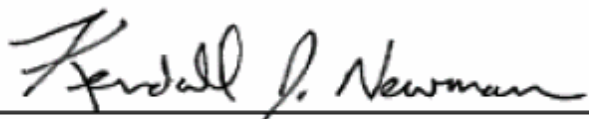
22. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

/s/ Heriberto Cadena

Heriberto Cadena
Special Agent
FBI

Subscribed and sworn to before me on: 10/18/2021


KENDALL J. NEWMAN
UNITED STATES MAGISTRATE JUDGE

/s/ Paul Hemesath
Approved as to form by AUSA PAUL HEMESATH

VI. CONCLUSION

22. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



Heriberto Cadena
Special Agent
FBI

Subscribed and sworn to before me on: 10/18/2021

Approved telephonically at 3:45 pm
The Honorable Jeremy D. Peterson
UNITED STATES MAGISTRATE JUDGE

/s/ Paul Hemesath
Approved as to form by AUSA PAUL HEMESATH

ATTACHMENT A

The property to be searched is a A MAC BOOK PRO, SERIAL NUMBER: C02PXMFCG8WN; AND AN IPHONE, SERIAL NUMBER: G6TX31CCJCL8, hereinafter the “Devices.” The Devices are currently located at A STORAGE LOCKER IN THE UNITED STATES PROBATION OFFICE IN ELK GROVE, CALIFORNIA.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of 18 U.S.C. §§ 1030(a)(5)(A), 1030(c)(4)(C) – knowingly causing the transmission of a program information code, or command, and as a result of such conduct, intentionally causes damage without authorization to a protected computer and involve Matthew Keys:

- a. any information pertaining to the access of any websites or services related to Comstock’s Magazine;
- b. any information concerning the unauthorized access of any Internet service;
- c. Any information pertaining to research and/or methodology concerning how to access delete data services hosted on the Intranet, including, but not limited to: YouTube channels, websites, email, company websites, and metadata concerning the same;
- d. Any information demonstrating attribution of the activity and/or data to a personal identity;
- e. Time/date/destination evidence of any Internet traffic from January 23 through March 11, 2020, and
- f. any information involving the location of the Devices from January 23 through March 11, 2020.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Records evidencing the use of the Devices connections with any servers through the Internet, including:

- a. records of Internet Protocol addresses used;
- b. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

4. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support

staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the

Eastern District of California

In the Matter of the Search of

A MAC BOOK PRO, SERIAL NUMBER:)
 C02PXMXXCG8WN; AND AN IPHONE, SERIAL)
 NUMBER: G6TX31CCJCL8, CURRENTLY)
 LOCATED AT A STORAGE LOCKER IN THE)
 UNITED STATES PROBATION OFFICE IN ELK)
 GROVE, CALIFORNIA)

Case No. 2:21-sw-0800 KJN

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of California
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A, attached hereto and incorporated by reference.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized):*

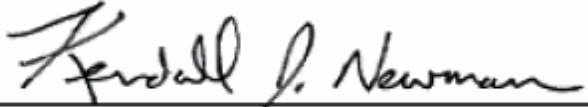
SEE ATTACHMENT B, attached hereto and incorporated by reference.**YOU ARE COMMANDED** to execute this warrant on or before 11/1/2021 *(not to exceed 14 days)*
☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to: any authorized U.S. Magistrate Judge in the Eastern District of California.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of .
Date and time issued: 10/18/2021 @ 3:45 pmCity and state: Sacramento, California


KENDALL J. NEWMAN
 UNITED STATES MAGISTRATE JUDGE

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		
Certification		
<p>I swear that this inventory is a true and detailed account of the person or property taken by me on the warrant.</p> <div style="margin-top: 20px;"><div style="border-bottom: 1px solid black; width: 60%; margin-left: auto; margin-right: auto;"></div><p style="text-align: center;">Subscribed, sworn to, and returned before me this date.</p><div style="margin-top: 20px;"><div style="border-bottom: 1px solid black; width: 50%; margin-left: auto; margin-right: auto;"></div><div style="display: flex; justify-content: space-between; margin-top: 10px;"><div style="width: 60%;"><div style="border-bottom: 1px solid black; width: 100%;"></div><div style="text-align: center;">Signature of Judge</div></div><div style="width: 35%;"><div style="border-bottom: 1px solid black; width: 100%;"></div><div style="text-align: center;">Date</div></div></div></div></div>		

ATTACHMENT A

The property to be searched is a A MAC BOOK PRO, SERIAL NUMBER: C02PXMFCG8WN; AND AN IPHONE, SERIAL NUMBER: G6TX31CCJCL8, hereinafter the “Devices.” The Devices are currently located at A STORAGE LOCKER IN THE UNITED STATES PROBATION OFFICE IN ELK GROVE, CALIFORNIA.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of 18 U.S.C. §§ 1030(a)(5)(A), 1030(c)(4)(C) – knowingly causing the transmission of a program information code, or command, and as a result of such conduct, intentionally causes damage without authorization to a protected computer and involve Matthew Keys:

- a. any information pertaining to the access of any websites or services related to Comstock’s Magazine;
- b. any information concerning the unauthorized access of any Internet service;
- c. Any information pertaining to research and/or methodology concerning how to access delete data services hosted on the Intranet, including, but not limited to: YouTube channels, websites, email, company websites, and metadata concerning the same;
- d. Any information demonstrating attribution of the activity and/or data to a personal identity;
- e. Time/date/destination evidence of any Internet traffic from January 23 through March 11, 2020, and
- f. any information involving the location of the Devices from January 23 through March 11, 2020.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Records evidencing the use of the Devices connections with any servers through the Internet, including:

- a. records of Internet Protocol addresses used;
- b. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

4. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support

staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.